80

Notice of Allowability	**Application No.** 09/892,242	**Applicant(s)** QI ET AL.	
	Examiner Ponnoreay Pich	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *9/25/07*.

2. ☒ The allowed claim(s) is/are *1,4-6,13-19,21,23,26-34,36,38,41-43*.

3. □ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) □ All b) □ Some* c) □ None of the:
   1. □ Certified copies of the priority documents have been received.
   2. □ Certified copies of the priority documents have been received in Application No. _____.
   3. □ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. □ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. □ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) □ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
   1) □ hereto or 2) □ to Paper No./Mail Date _____.
   (b) □ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. □ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. □ Notice of References Cited (PTO-892)
2. □ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. □ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. □ Notice of Informal Patent Application
6. □ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. □ Other _____.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Lori Gordon (Reg. No. 50,633) on 11/27/07. The amendments are to fix typo's and minor informalities. As the substance of the interview has been summarized herein, a separate interview summary form is not provided (see MPEP 713.04).

The application has been amended as follows:

AMEND THE FOLLOWING CLAIMS:

1. (currently amended) A DES cryptography engine for performing cryptographic operations on a data block, the cryptography engine comprising:

a key scheduler configured to provide keys for cryptographic operations;

eight bit-slice modules, each bit-slice module including:

first circuitry configured to perform an exclusive OR (XOR) on a first bit sequence and a portion of a key provided by the key scheduler to generate a second bit sequence;

a DES substitution box (SBox) configured to transform the second bit sequence into a third bit sequence;

second circuitry configured to perform an exclusive OR (XOR) on the third bit sequence and a left portion of an input bit sequence for the current cryptographic round to generate a fourth bit sequence,

wherein the fourth bit sequence is a right portion of an output bit sequence and a right portion of the input bit sequence is a left portion of the output bit sequence of a current DES round for the bit [[slide]] slice module;

permutation logic configured to receive the fourth bit sequence from each of the eight bit-slice modules and to perform a permutation on the received fourth bit sequences; and

expansion logic configured to generate a set of first bit sequences by expanding received bit sequences and to provide a first bit sequence to each bit slice module.

23. (currently amended) An integrated circuit [[layout]] associated with a DES cryptography engine for performing cryptographic operations on a data block, the integrated circuit [[layout]] providing information for configuring the DES cryptography engine, the integrated circuit [[layout]] comprising:

a key scheduler configured to provide keys for cryptographic operations;

eight bit-slice modules, each bit-slice module including:

first circuitry configured to perform an exclusive OR (XOR) on a first bit sequence and a portion of a key provided by the key scheduler to generate a second bit sequence;

a DES substitution box (SBox) configured to transform the second bit sequence into a third bit sequence;

second circuitry configured to perform an exclusive OR (XOR) on the third bit sequence and a left portion of an input bit sequence for the current cryptographic round to generate a fourth bit sequence,

wherein the fourth bit sequence is a right portion of an output bit sequence and a right portion of the input bit sequence is a left portion of the output bit sequence of a current DES round for the bit [[slide]] slice module;

permutation logic configured to receive the fourth bit sequence from each of the eight bit-slice modules and to perform a permutation on the received fourth bit sequences; and

expansion logic configured to generate a set of first bit sequences by expanding received bit sequences and to provide a first bit sequence to each bit slice module.

26. (currently amended) The integrated circuit [[layout]] of claim 23 wherein each bit-slice module further comprises two-level multiplexer circuitry, wherein a first level of the two-level multiplexer is configured to receive an inverse permutation of a first portion of an initial input bit sequence and an inverse permutation of a second portion of the input bit sequence during an initial cryptographic round and the left portion of the output bit sequence from a previous cryptographic round during a subsequent cryptographic round and wherein a second level of the two-level multiplexer is configured to receive the output of the first level and the right portion of the output bit sequence generated during the previous cryptographic round.

27. (currently amended) The integrated circuit [[layout]] of claim 23, wherein the first and second bit sequences are four bits.

28. (currently amended) The integrated circuit [[layout]] of claim 27, wherein the third and fourth bit sequences are six bits.

29. (currently amended) The integrated circuit [[layout]] of claim 23, wherein the key scheduler performs pipelined key scheduling logic.

30. (currently amended) The integrated circuit [[layout]] of claim 23, wherein the key scheduler comprises a determination stage.

31. (currently amended) The integrated circuit [[layout]] of claim 23, wherein the key scheduler comprises a shift stage.

32. (currently amended) The integrated circuit [[layout]] of claim 23, wherein the key scheduler comprises a propagation stage.

33. (currently amended) The integrated circuit [[layout]] of claim 23, wherein the key scheduler comprises a consumption stage.

34. (currently amended) The integrated circuit [[layout]] of claim 23, wherein a first shift amount for a first key is identified in a determination stage using a first round counter value.

36. (currently amended) The integrated circuit [[layout]] of claim 26 , wherein the two-level multiplexer is configured to swap the left portion of the output bit sequence of a previous cryptographic round with the right portion of the output bit sequence of the

previous cryptographic round, whereby the right portion of the input bit sequence of the previous cryptographic round becomes the left portion of an input bit sequence for the current cryptographic round and the fourth bit sequence becomes a right portion of the input bit sequence for the current cryptographic round.

The following is an examiner's statement of reasons for allowance: Applicant's amendments to the independent claims have overcome prior art. As per independent claim 1, the prior art does not teach a DES cryptography engine having:

eight bit-slice modules, each bit-slice module including:

first circuitry configured to perform an exclusive OR (XOR) on a first bit sequence and a portion of a key provided by the key scheduler to generate a second bit sequence;

a DES substitution box (SBox) configured to transform the second bit sequence into a third bit sequence;

second circuitry configured to perform an exclusive OR (XOR) on the third bit sequence and a left portion of an input bit sequence for the current cryptographic round to generate a fourth bit sequence,

wherein the fourth bit sequence is a right portion of an output bit sequence and a right portion of the input bit sequence is a left portion of the output bit sequence of a current DES round for the bit slice module;

permutation logic configured to receive the fourth bit sequence from each of the eight bit-slice modules and to perform a permutation on the received fourth bit sequences.

Claim 23 contains similar limitations as claim 1.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Thurs.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Ponnoreay Pich
Examiner
Art Unit 2135

PP

KIM VU
PATENT EXAMINER
CENTER 2100